

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO**

CINDY WESTMAN, individually and as next friend of **Z.R.**, a minor, and on behalf of all others similarly situated,

Plaintiffs,

v.

**PRENTKE ROMICH COMPANY
d/b/a PRC-SALTIMBO,**

Defendant.

Case No. 5:24-cv-01738

CLASS ACTION COMPLAINT

Plaintiff Cindy Westman, on behalf of herself and her minor child, Z.R. (“Plaintiffs”) and all similarly situated persons, allege the following against Prentke Romich Company d/b/a PRC-Saltillo (“PRC-Saltillo” or “Defendant”) based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiffs’ counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against PRC-Saltillo for its failure to properly secure and safeguard Plaintiffs’ and other similarly situated PRC-Saltillo customers’ personally identifiable information (“PII”) and protected health information (“PHI”), including names, addresses, phone numbers, dates of birth, treatment cost information, referring/treating physician, health insurance policy numbers, Medicare/Medicaid plan names, and/or medical device purchased (the “Private Information”), from criminal hackers.

2. PRC-Saltillo, which is based in Wooster, Ohio, is a worldwide developer of speech-generating devices (SGDs), market-leading apps and several innovative AAC language systems that enable individuals with complex communication disorders the ability to express themselves.

3. On or about September 12, 2024, PRC-Saltillo filed official notice of a hacking incident with the Office of the Maine Attorney General. Under state and federal law, organizations must report breaches involving PHI within at least sixty (60) days.

4. On or about September 25, 2024, PRC-Saltillo also sent out data breach letters (the “Notice”) to individuals whose information was compromised as a result of the hacking incident.

5. Based on the Notice sent to Plaintiffs and “Class Members” (defined below), unusual activity was detected on some of its computer systems. In response, Defendant initiated an investigation. PRC-Saltillo’s investigation revealed that an unauthorized party had access to certain files that contained sensitive customer information, and that such access took place between August 13, 2024, and August 21, 2024 (the “Data Breach”).

6. Plaintiffs and “Class Members” (defined below) were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. The Private Information compromised in the Data Breach contained highly sensitive customer data, representing a gold mine for data thieves. The data included, but is not limited to, treatment cost information, referring/treating physician, health insurance policy numbers, Medicare/Medicaid plan names, and/or medical device purchased that PRC-Saltillo collected and maintained in its ordinary course of business.

8. Armed with the Private Information accessed in the Data Breach (and a head start), data thieves can commit a variety of crimes including, *e.g.*, using Class Members’ names to obtain

medical services, using Class Members' information to obtain government benefits, and giving false information to police during an arrest.

9. There has been no assurance offered by PRC-Saltillo that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

10. Perhaps most troubling, in mid-September, ransomware gang Fog posted the company to its data leak site, alleging to have stolen 250GB of data.¹

11. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

12. Plaintiffs bring this class action lawsuit to address PRC-Saltillo's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

13. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to PRC-Saltillo, and thus PRC-Saltillo was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

14. Upon information and belief, PRC-Saltillo failed to properly implement security practices with regard to the computer network and systems that housed the Private Information. Had PRC-Saltillo properly monitored its networks, it would have discovered the Breach sooner.

¹ See HookPhish, *Ransomware [FOG] – Group Hits: Prentke Romich Company* (Sept. 18, 2024), <https://www.hookphish.com/blog/ransomware-fog-group-hits-prentke-romich-company/> (last accessed October 7, 2024).

15. Plaintiffs' and Class Members' identities are now at risk because of PRC-Saltillo's negligent conduct, resulting in the Private Information that PRC-Saltillo collected and maintained being stolen by known data thieves and other unauthorized third parties.

16. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

17. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for negligence, negligence *per se*, breach of express contract, breach of implied contract, violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, unjust enrichment, breach of fiduciary duty, breach of confidence, and declaratory judgment.

II. PARTIES

18. Plaintiff Cindy Westman and her minor child are, and at all times mentioned herein were, individual citizens of the State of Illinois.

19. Defendant PRC-Saltillo is a technology and manufacturing company incorporated in Ohio with its principal place of business at 1022 Heyl Rd, Wooster, Ohio 44691 in Wayne County.

III. JURISDICTION AND VENUE

20. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from PRC-Saltillo. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

21. This Court has jurisdiction over PRC-Saltillo because PRC-Saltillo operates in and/or is incorporated in this District.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1331(a)(1) because a substantial part of the events giving rise to this action occurred in this District and PRC-Saltillo has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. *PRC-Saltillo's Business and Collection of Plaintiffs' and Class Members' Private Information*

23. PRC-Saltillo is a technology and manufacturing. Founded in 1966, PRC-Saltillo develops speech-generating devices, apps and several innovative Augmentative and Alternative Communication (“AAC”) language systems designed to give individuals with complex communication disorders the ability to express themselves. Upon information and belief, PRC-Saltillo employs more than 247 people and generates approximately \$62 million in annual revenue.

24. As a condition of receiving communication assistance devices and services, PRC-Saltillo requires that its customers entrust it with highly sensitive personal and health information. In the ordinary course of receiving service from PRC-Saltillo, Plaintiffs and Class Members were required to provide their Private Information to Defendant.

25. In its Notice of Privacy Practices, PRC-Saltillo promises its customers that “PRC-Saltillo respects your right to privacy and the security of your information.” and says that it only “collects, uses and discloses your information, including PHI, in accordance with applicable law”² PRC-Saltillo also describes in its Privacy Policy the limited specific instances when it shares

² See PRC-Saltillo, *Notice of Privacy Practices* (effective Dec. 9, 2020), https://www.prc-saltillo.com/assets/uploads/PRC-Saltillo_Privacy_Policy_120920.pdf (last visited Oct. 7, 2024).

customer health information and says that it will otherwise share customers' information "only authorized by you."³

26. Thus, due to the highly sensitive and personal nature of the information PRC-Saltillo acquires and stores with respect to its customers, PRC-Saltillo, upon information and belief, promises to, among other things: keep customers' Private Information private; comply with industry standards related to data security and the maintenance of its customers' Private Information; inform its customers of its legal duties relating to data security and comply with all federal and state laws protecting customers' Private Information; only use and release customers' Private Information for reasons that relate to the services it provides; and provide adequate notice to customers if their Private Information is disclosed without authorization.

27. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, PRC-Saltillo assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

28. Plaintiffs and Class Members relied on PRC-Saltillo to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

B. The Data Breach and Defendant's Inadequate Notice to Plaintiffs and Class Members

29. According to Defendant's Notice, it learned of unauthorized access to its computer systems on or about August 21, 2024, with such unauthorized access having taken place between August 14, 2024 and August 21, 2024.

³ *Id.*

30. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including names, addresses, phone numbers, dates of birth, treatment cost information, referring/treating physician, health insurance policy numbers, Medicare/Medicaid plan names, and/or medical device purchased.

31. On or about September 25, 2024, roughly one month after PRC-Saltillo learned that the Class's Private Information was first accessed by cybercriminals, PRC-Saltillo finally began to notify customers that its investigation determined that their Private Information was affected.

32. PRC-Saltillo had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

33. Plaintiffs and Class Members provided their Private Information to PRC-Saltillo with the reasonable expectation and mutual understanding that PRC-Saltillo would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

34. PRC-Saltillo's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

35. PRC-Saltillo knew or should have known that its electronic records would be targeted by cybercriminals.

C. The Healthcare Sector is Particularly Susceptible to Data Breaches

36. PRC-Saltillo was on notice that companies in the healthcare industry are susceptible targets for data breaches.

37. PRC-Saltillo was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems,

Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that “[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI).”⁴

38. The American Medical Association (“AMA”) has also warned healthcare companies about the importance of protecting their patients’ confidential information:

Cybersecurity is not just a technical issue; it’s a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients’ health and financial information, but also patient access to care.⁵

39. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.⁶ In 2022, the largest growth in compromises occurred in the healthcare sector.⁷

40. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the “average total cost to resolve an identity theft-related incident . . . came to about \$20,000,” and that the victims

⁴ Jim Finkle, *FBI warns healthcare firms they are targeted by hackers*, Reuters (Aug. 20, 2014), <https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820> (last visited Oct. 7, 2024).

⁵ Andis Robežnieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass’n. (Oct. 4, 2019), <https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals> (last visited Oct. 7, 2024).

⁶ Identity Theft Resource Center, *2018 End-of-Year Data Breach Report* (Jan. 28, 2019), archived at https://web.archive.org/web/20190823232406/https://www.idtheftcenter.org/wp-content/uploads/2019/01/ITRC_2018-EOY-Breach-Report-Key-Findings.pdf (last visited Oct. 7, 2024).

⁷ Identity Theft Resource Center, *2022 End-of-Year Data Breach Report*, at 11, https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited Oct. 7, 2024).

were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.⁸

41. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.⁹

42. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. “Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.”¹⁰

43. As a healthcare device and services provider, PRC-Saltillo knew, or should have known, the importance of safeguarding its customers’ Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on PRC-Saltillo’s customers as a result of a breach. PRC-Saltillo failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

⁸ Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), <https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/> (last visited Oct. 7, 2024).

⁹ *Id.*

¹⁰ Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, Chief Healthcare Executive (Apr. 4, 2019), <https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks> (last visited Oct. 7, 2024).

D. PRC-Saltillo Failed to Comply with HIPAA

44. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See 42 U.S.C. §§ 1301, et seq.* These provisions require that the Department of Health and Human Services (“HHS”) create rules to streamline the standards for handling PHI similar to the data Defendant left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

45. PRC-Saltillo’s Data Breach resulted from a combination of insufficiencies that indicate PRC-Saltillo failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from PRC-Saltillo’s Data Breach that PRC-Saltillo either failed to implement, or inadequately implemented, information security policies or procedures to protect Plaintiffs’ and Class Members’ PHI.

46. Plaintiffs’ and Class Members’ Private Information compromised in the Data Breach included “protected health information” as defined by CFR § 160.103.

47. 45 CFR § 164.402 defines “breach” as “the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.”

48. 45 CFR § 164.402 defines “unsecured protected health information” as “protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]”

49. Plaintiffs’ and Class Members’ Private Information included “unsecured protected health information” as defined by 45 CFR § 164.402.

50. Plaintiffs’ and Class Members’ unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

51. Based upon Defendant's Notice to Plaintiffs and Class Members, PRC-Saltillo reasonably believes that Plaintiffs' and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

52. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

53. PRC-Saltillo reasonably believes that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

54. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

55. Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

56. PRC-Saltillo reasonably believes that Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

57. It is reasonable to infer that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as

a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

58. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

59. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

60. In addition, PRC-Saltillo's Data Breach could have been prevented if PRC-Saltillo had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its customers.

61. PRC-Saltillo's security failures also include, but are not limited to:

- a. Failing to maintain an adequate data security system to prevent data loss;
- b. Failing to mitigate the risks of a data breach and loss of data;
- c. Failing to ensure the confidentiality and integrity of electronic protected health information PRC-Saltillo creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);
- d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only

to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

- e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);
- f. Failing to identify and respond to suspected or known security incidents;
- g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);
- h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);
- i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);
- j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and
- k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

62. Because PRC-Saltillo has failed to comply with HIPAA, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is also necessary to ensure PRC-Saltillo's approach to information security is adequate and appropriate going forward. PRC-Saltillo still maintains the PHI and other highly sensitive PII of its current and former customers,

including Plaintiffs and Class Members. Without the supervision of the Court through injunctive relief, Plaintiffs' and Class Members' Private Information remains at risk of subsequent data breaches.

E. PRC-Saltillo Failed to Comply with FTC Guidelines

63. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. *See, e.g.,* *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

64. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network’s vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

65. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for

suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

66. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

67. As evidenced by the Data Breach, PRC-Saltillo failed to properly implement basic data security practices. PRC-Saltillo's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

68. PRC-Saltillo was at all times fully aware of its obligation to protect the Private Information of its customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. PRC-Saltillo Failed to Comply with Industry Standards

69. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

70. Some industry best practices that should be implemented by businesses dealing with sensitive PHI like PRC-Saltillo include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees

can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

71. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

72. Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR-AA-01, PR-AA-02, PR-AA-03, PR-AA-04, PR-AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiffs' and Class Members' Private Information, resulting in the Data Breach.

73. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

G. PRC-Saltillo Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information

74. In addition to its obligations under federal and state laws, PRC-Saltillo owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. PRC-Saltillo owed a

duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

75. PRC-Saltillo breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. PRC-Saltillo's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect customers' Private Information;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to sufficiently train its employees regarding the proper handling of its customers' Private Information;
- e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;
- f. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and
- g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

76. PRC-Saltillo negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

77. Had PRC-Saltillo remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

78. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with PRC-Saltillo.

H. PRC-Saltillo Should Have Known that Cybercriminals Target PII and PHI to Carry Out Fraud and Identity Theft

79. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.¹¹ Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

80. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

¹¹ Fed. Trade Comm'n, *FTC Information Injury Workshop: BE and BCP Staff Perspective* (Oct. 2018), https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-oct_2018_0.pdf (last visited Oct. 7, 2024).

81. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

82. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

83. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

84. One such example of this is the development of "Fullz" packages.

85. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

86. The development of “Fullz” packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs’ and the proposed Class’s phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members’ stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

87. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim’s identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.¹² However, these steps do not guarantee protection from identity theft but can only mitigate identity theft’s long-lasting negative impacts.

88. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud.

¹² See Fed. Trade Comm’n, *What To Do Right Away, What To Do Next*, IdentityTheft.gov, <https://www.identitytheft.gov/Steps> (last visited Oct. 7, 2024).

89. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.¹³

90. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

91. While credit card information and associated PII can sell for as little as \$1-\$2 on the black market, protected health information can sell for as much as \$363 according to the Infosec Institute.¹⁴

92. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

93. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."¹⁵

¹³ Fed. Trade Comm'n, *Warning Signs of Identity Theft*, <https://consumer.ftc.gov/articles/what-know-about-identity-theft> (last visited Oct. 7, 2024).

¹⁴ Center for Internet Security, *Data Breaches: In the Healthcare Sector*, <https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector> (last visited Oct. 7, 2024).

¹⁵ Michael Ollove, *The Rise Of Medical Identity Theft In Healthcare*, KFF Health News (Feb. 7, 2014), <https://kffhealthnews.org/news/rise-of-indentity-theft/> (last visited Oct. 7, 2024).

94. The ramifications of PRC-Saltillo's failure to keep its customers' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

95. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

96. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:¹⁶

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

97. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

98. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

¹⁶ U.S. Gov't Accountability Off., *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Oct. 7, 2024).

I. Plaintiffs' and Class Members' Damages

Plaintiff Westman's and Z.R.'s Experience

99. Plaintiff Westman and her minor child, Z.R., are customers of PRC-Saltillo.

100. When Plaintiffs became customers, Defendant required Plaintiff Westman provide it with substantial amounts of her and Z.R.'s Private Information, including PHI.

101. On or about September 25, 2024, Plaintiff Westman received the Notice, which told her that Z.R.'s Private Information had been affected during the Data Breach. The Notice informed her that the Private Information stolen included Z.R.'s "name, phone number, address, date of birth, treatment cost information, referring/treating physician, health insurance policy number, Medicare/Medicaid plan name, and/or medical device purchased."

102. The Notice offered Plaintiff Westman only generic steps she and Z.R. could take to protect themselves. This is not sufficient given that Plaintiff Westman and her minor child, Z.R., will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

103. Plaintiff Westman suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her and her minor child's medical, health insurance, and other accounts for fraud.

104. Plaintiff Westman would not have provided her or her minor child, Z.R.'s, Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its customers' personal and health information from theft, and that those systems were subject to a data breach.

105. Z.R. suffered actual injury in the form of having her PII and PHI compromised and/or stolen as a result of the Data Breach.

106. Z.R. also suffered actual injury in the form of damages to and diminution in the value of her personal, health, and financial information – a form of intangible property that was entrusted to Defendant for the purpose of receiving healthcare-related devices and services from Defendant and which was compromised in, and as a result of, the Data Breach.

107. Z.R. suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals, including but not limited to, the Fog ransomware group.

108. Plaintiff Westman and her minor child, Z.R., have a continuing interest in ensuring that their PII and PHI, which remain in the possession of Defendant, is protected and safeguarded from future breaches.

109. As a result of the Data Breach, Plaintiff Westman has had to make reasonable efforts to mitigate the impact of the Data Breach on her life and that of her minor child, including but not limited to, researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the steps offered by Defendant in its Notice. Plaintiff Westman has spent several hours dealing with the Data Breach – valuable time she otherwise would have spent on other activities.

110. As a result of the Data Breach, Plaintiff Westman has suffered anxiety as a result of the release of her minor child's Private Information, which she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her minor child's PII and PHI for purposes of committing cyber and other crimes against her and her minor child. Plaintiff Westman is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and

fraud resulting from the Data Breach would have on her and her minor child's life for many years to come.

111. Z.R. also suffered actual injury from having her Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff []; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

112. As a result of the Data Breach, Plaintiff Westman anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

113. In sum, Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

114. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

115. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

116. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

117. Plaintiffs and Class Members also lost the benefit of the bargain they made with PRC-Saltillo. Plaintiffs and Class Members overpaid for medical devices and services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiffs and Class Members paid to PRC-Saltillo (and/or that was paid on their behalf) was intended to be used by PRC-Saltillo to fund adequate security of PRC-Saltillo's system and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class did not receive the benefit of the bargain.

118. Additionally, Z.R. suffered a loss of value of her Private Information when it was acquired by cyber thieves, like Fog, in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly \$200 billion.¹⁷ In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to \$60 a year.¹⁸

119. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

¹⁷ See The Quantum Record, *How Data Brokers Profit from the Data We Create* (Apr. 25, 2023), <https://thequantumrecord.com/blog/data-brokers-profit-from-our-data> (last visited Oct. 7, 2024).

¹⁸ The Nielsen Company (US), LLC, Nielsen Computer & Mobile Panel, *Frequently Asked Questions: What Rewards Can I Earn?*, <https://computermobilepanel.nielsen.com/ui/US/en/faqen.html> (last visited Oct. 7, 2024).

120. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

121. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of PRC-Saltillo, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal and health information of its customers is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

122. As a direct and proximate result of PRC-Saltillo's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

123. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

124. Specifically, Plaintiffs propose the following Nationwide Class, as well as the following State Subclass definitions (collectively referred to herein as the "Class"), subject to amendment as appropriate:

Nationwide Class

All individuals in the United States who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

Illinois Subclass

All residents of Illinois who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

125. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

126. Plaintiffs reserve the right to modify or amend the definitions of the proposed Nationwide Class, as well as the Illinois Subclass, before the Court determines whether certification is appropriate.

127. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

128. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of 51,600 customers of PRC-Saltillo whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through PRC-Saltillo's records, Class Members' records, publication notice, self-identification, and other means.

129. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether PRC-Saltillo engaged in the conduct alleged herein;
- b. Whether PRC-Saltillo's conduct violated the FTCA, HIPAA, and/or the Illinois Consumer Fraud and deceptive Business Practices Act;

- c. When PRC-Saltillo learned of the Data Breach;
- d. Whether PRC-Saltillo's response to the Data Breach was adequate;
- e. Whether PRC-Saltillo unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;
- f. Whether PRC-Saltillo failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;
- g. Whether PRC-Saltillo's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- h. Whether PRC-Saltillo's data security systems prior to and during the Data Breach were consistent with industry standards;
- i. Whether PRC-Saltillo owed a duty to Class Members to safeguard their Private Information;
- j. Whether PRC-Saltillo breached its duty to Class Members to safeguard their Private Information;
- k. Whether hackers obtained Class Members' Private Information via the Data Breach;
- l. Whether PRC-Saltillo had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;
- m. Whether PRC-Saltillo breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;
- n. Whether PRC-Saltillo knew or should have known that its data security systems and monitoring processes were deficient;

- o. What damages Plaintiffs and Class Members suffered as a result of PRC-Saltillo's misconduct;
- p. Whether PRC-Saltillo's conduct was negligent;
- q. Whether PRC-Saltillo's conduct was *per se* negligent;
- r. Whether PRC-Saltillo was unjustly enriched;
- s. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;
- t. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and
- u. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

130. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of PRC-Saltillo. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

131. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

132. Predominance. PRC-Saltillo has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from PRC-Saltillo's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

133. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for PRC-Saltillo. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

134. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). PRC-Saltillo has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

135. Finally, all members of the proposed Class are readily ascertainable. PRC-Saltillo has access to the names and addresses and/or email addresses of Class Members affected by the

Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by PRC-Saltillo.

CLAIMS FOR RELIEF

**COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR
ALTERNATIVELY THE ILLINOIS SUBCLASS)**

136. Plaintiffs restate and reallege all allegations stated above as if fully set forth herein.

137. PRC-Saltillo knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

138. PRC-Saltillo knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. PRC-Saltillo was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

139. PRC-Saltillo owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. PRC-Saltillo's duties included, but were not limited to, the following:

- a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;
- b. To protect customers' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;
- c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

- d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to HIPAA, the FTCA and Illinois Consumer Fraud and Deceptive Business Practices Act;
- e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and
- f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

140. PRC-Saltillo's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

141. PRC-Saltillo's duty also arose because Defendant was bound by industry standards to protect its customers' confidential Private Information.

142. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and PRC-Saltillo owed them a duty of care to not subject them to an unreasonable risk of harm.

143. PRC-Saltillo, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within PRC-Saltillo's possession.

144. PRC-Saltillo, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

145. PRC-Saltillo breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to comply with the FTCA; and
- f. Failing to detect in a timely manner that Class Members' Private Information had been compromised.

146. PRC-Saltillo had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust PRC-Saltillo with their Private Information was predicated on the understanding that PRC-Saltillo would take adequate security precautions. Moreover, only PRC-Saltillo had the ability to protect its systems (and the Private Information that it stored on them) from attack.

147. PRC-Saltillo's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised and exfiltrated, as alleged herein.

148. PRC-Saltillo's breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

149. As a result of PRC-Saltillo's negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

150. PRC-Saltillo also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

151. As a direct and proximate result of PRC-Saltillo's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

152. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

153. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

154. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring PRC-Saltillo to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
NEGLIGENCE *PER SE*
**(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR
ALTERNATIVELY THE ILLINOIS SUBCLASS)**

155. Plaintiffs restate and reallege all allegations stated above as if fully set forth herein.

156. Pursuant to Section 5 of the FTCA, PRC-Saltillo had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

157. Pursuant to HIPAA, 42 U.S.C. § 1302(d), *et seq.*, PRC-Saltillo had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

158. Specifically, pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

159. PRC-Saltillo breached its duties to Plaintiffs and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

160. Specifically, PRC-Saltillo breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

161. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of PRC-Saltillo's duty in this regard.

162. PRC-Saltillo also violated the FTCA and HIPAA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

163. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to PRC-Saltillo's networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

164. Plaintiffs and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect and PRC-Saltillo's failure to comply with both constitutes negligence *per se*.

165. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to PRC-Saltillo's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

166. As a direct and proximate result of PRC-Saltillo's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

167. As a direct and proximate result of PRC-Saltillo's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

168. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring PRC-Saltillo to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
BREACH OF CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR
ALTERNATIVELY THE ILLINOIS SUBCLASS)

169. Plaintiffs restate and reallege all allegations stated above as if fully set forth herein.

170. Plaintiffs and Class Members entered into a valid and enforceable contract through which they paid money to PRC-Saltillo in exchange for services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiffs' and Class Members' Private Information.

171. PRC-Saltillo's Privacy Policy memorialized the rights and obligations of PRC-Saltillo and its customers. This document was provided to Plaintiffs and Class Members in a manner in which it became part of the agreement for services.

172. In the Privacy Policy, PRC-Saltillo commits to protecting the privacy and security of private information and promises to never share Plaintiffs' and Class Members' Private Information except under certain limited circumstances.

173. Plaintiffs and Class Members fully performed their obligations under their contracts with PRC-Saltillo.

174. However, PRC-Saltillo did not secure, safeguard, and/or keep private Plaintiffs' and Class Members' Private Information, and therefore PRC-Saltillo breached its contracts with Plaintiffs and Class Members.

175. PRC-Saltillo allowed third parties to access, copy, and/or exfiltrate Plaintiffs' and Class Members' Private Information without permission. Therefore, PRC-Saltillo breached the Privacy Policy with Plaintiffs and Class Members.

176. PRC-Saltillo's failure to satisfy its confidentiality and privacy obligations, specifically those arising under the FTCA, HIPAA, and applicable industry standards, resulted in PRC-Saltillo providing services to Plaintiffs and Class Members that were of a diminished value.

177. As a result, Plaintiffs and Class Members have been harmed, damaged, and/or injured as described herein, including in Defendant's failure to fully perform its part of the bargain with Plaintiffs and Class Members.

178. As a direct and proximate result of PRC-Saltillo's conduct, Plaintiffs and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

179. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring PRC-Saltillo to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT IV
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR
ALTERNATIVELY THE ILLINOIS SUBCLASS)

180. Plaintiffs restate and reallege all allegations stated above as if fully set forth herein.

181. This Count is pleaded in the alternative to Count III above.

182. PRC-Saltillo provides communication assistance devices to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiffs and Class Members paying for services and/or entrusting their valuable Private Information to Defendant in exchange for such services.

183. Through Defendant's sale of products and services to Plaintiffs and Class Members, it knew or should have known that it must protect Plaintiffs' and Class Members' confidential Private Information in accordance with its policies, practices, and applicable law.

184. As consideration, Plaintiffs and Class Members paid money to PRC-Saltillo and/or turned over valuable Private Information to PRC-Saltillo. Accordingly, Plaintiffs and Class Members bargained with PRC-Saltillo to securely maintain and store their Private Information.

185. PRC-Saltillo accepted payment and/or possession of Plaintiffs' and Class Members' Private Information for the purpose of providing devices and services to Plaintiffs and Class Members.

186. In paying Defendant and/or providing their valuable Private Information to Defendant in exchange for Defendant's devices and services, Plaintiffs and Class Members intended and understood that PRC-Saltillo would adequately safeguard the Private Information as part of those services.

187. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; (7) complying with HIPAA standards to make sure that Plaintiffs' and Class Members' PHI would remain protected; and (8) taking other steps to protect against foreseeable data breaches.

188. Plaintiffs and Class Members would not have entrusted their Private Information to PRC-Saltillo in the absence of such an implied contract.

189. Had PRC-Saltillo disclosed to Plaintiffs and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their Private Information to PRC-Saltillo.

190. As a provider of healthcare related devices and services, PRC-Saltillo recognized (or should have recognized) that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and the other Class Members.

191. PRC-Saltillo violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information. PRC-Saltillo further breached these implied contracts by failing to comply with its promise to abide by HIPAA.

192. Additionally, PRC-Saltillo breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

193. PRC-Saltillo also breached the implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

194. PRC-Saltillo further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

195. PRC-Saltillo further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

196. PRC-Saltillo further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2).

197. PRC-Saltillo further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

198. PRC-Saltillo further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations, in violation of 45 CFR 164.306(a)(94).

199. PRC-Saltillo further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

200. PRC-Saltillo further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing

physical administrative safeguards to reasonably safeguard protected health information, in violation of 45 CFR 164.530(c).

201. PRC-Saltillo further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PHI.

202. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide payment and/or accurate and complete Private Information to PRC-Saltillo in exchange for PRC-Saltillo's agreement to, *inter alia*, provide services that included protection of their highly sensitive Private Information.

203. Plaintiffs and Class Members have been damaged by PRC-Saltillo's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT V
VIOLATION OF ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT
(ON BEHALF OF PLAINTIFFS AND THE ILLINOIS SUBCLASS)

204. Plaintiffs restate and reallege all allegations stated above as if fully set forth herein.

205. As fully alleged above, PRC-Saltillo engaged in unfair and deceptive acts and practices in violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. § 505/1, et seq. (the "CFA")

206. Reasonable individuals would be misled by PRC-Saltillo's misrepresentations and/or omissions concerning the security of their Private Information because they assume companies, like PRC-Saltillo, that collect PII and PHI from customers will properly safeguard such in a manner consistent with industry standards and practices.

207. PRC-Saltillo failed to inform Plaintiffs or Class Members of its inadequate data security practices and procedures that led to the Data Breach, thereby misleading Plaintiffs and

Class Members, in violation of §505/1 *et seq.* Such misrepresentations and/or omissions were material because Plaintiffs and Class Members entrusted PRC-Saltillo with their Private Information.

208. Had Plaintiffs and Class Members known of PRC-Saltillo's failure to maintain adequate security measures to protect their Private Information, they would not have entrusted their Private Information to Defendant.

209. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the provision of and advertisement of their services in violation of the CFA, including (a) failing to maintain adequate data security to keep Plaintiffs' and Class Members' Private Information from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTCA and HIPPA; (b) failing to disclose or omitting material facts to Plaintiffs and Class Members regarding Defendant's lack of adequate data security and inability or unwillingness to properly secure and protect the Private Information of Plaintiffs and Class members; (c) failing to disclose or omitting material facts to Plaintiffs and Class Members about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Private Information of Plaintiffs and Class Members; and (d) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs' and Class Members' Private Information from further unauthorized disclosure, release, data breaches, and theft.

210. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about its inadequate data security and its failure to comply with applicable state and federal laws and industry standards would be unknown and not easily

discoverable by Plaintiffs and Class Members and would defeat Plaintiffs' and Class Members' reasonable expectation about the security of their Private Information.

211. Defendant intended that Plaintiffs and Class Members would rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's provision of services.

212. Defendant's wrongful practices were and are injurious to the public because those practices were part of PRC-Saltillo's generalized course of conduct that applied to Plaintiffs and Class Members. Plaintiffs and Class Members have been adversely affected by PRC-Saltillo's conduct and the public was and is at risk thereof.

213. Defendant also violated 815 Ill. Comp. Stat. § 505/2 by failing to immediately notify Plaintiffs and Class Members of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 Ill. Comp. Stat. § 530/1.

214. As a result of LSSI's wrongful conduct, Plaintiffs and Class Members were injured in that they never would have provided their Private Information to PRC-Saltillo had they known or been told that PRC-Saltillo failed to maintain sufficient security to keep their Private Information from being hacked and taken and misused by others.

215. As a direct and proximate result of Defendant's violations of the CFA, Plaintiffs and Class Members have suffered harm, including identity theft, harm resulting from damaged credit scores and information, loss of time and money obtaining protections against future identity theft, loss of time and money resolving fraudulent charges, unreimbursed losses related to fraudulent charges, and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Private Information, entitling them to damages in an amount to be proven at trial.

216. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiffs and Class Members seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's CFA violations.

COUNT VI
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR
ALTERNATIVELY THE ILLINOIS SUBCLASS)

217. Plaintiffs restate and reallege all allegations stated above as if fully set forth herein.

218. This Count is pleaded in the alternative to Counts III and IV above.

219. Plaintiffs and Class Members conferred a benefit on PRC-Saltillo by turning over their Private Information to Defendant and by paying for products and services that should have included cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

220. Upon information and belief, PRC-Saltillo funds its data security measures entirely from its general revenue, including from payments made to it by Plaintiffs and Class Members.

221. As such, a portion of the payments made by Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to PRC-Saltillo.

222. PRC-Saltillo has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

223. PRC-Saltillo knew that Plaintiffs and Class Members conferred a benefit upon it, which PRC-Saltillo accepted. PRC-Saltillo profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the

payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

224. If Plaintiffs and Class Members had known that PRC-Saltillo had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

225. Due to PRC-Saltillo's conduct alleged herein, it would be unjust and inequitable under the circumstances for PRC-Saltillo to be permitted to retain the benefit of its wrongful conduct.

226. As a direct and proximate result of PRC-Saltillo's conduct, Plaintiffs and Class Members have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not limited to the following: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in PRC-Saltillo's possession and is subject to further unauthorized disclosures so long as PRC-Saltillo fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

227. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from PRC-Saltillo and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by PRC-Saltillo from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

228. Plaintiffs and Class Members may not have an adequate remedy at law against PRC-Saltillo, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VII
BREACH OF FIDUCIARY DUTY
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR
ALTERNATIVELY THE ILLINOIS SUBCLASS)

229. Plaintiffs restate and reallege all allegations stated above as if fully set forth herein.

230. In light of the special relationship between PRC-Saltillo and its customers, whereby PRC-Saltillo became a guardian of Plaintiffs' and Class Members' Private Information (including highly sensitive, confidential, personal, and other PHI) PRC-Saltillo was a fiduciary, created by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiffs and Class Members. This benefit included (1) the safeguarding of Plaintiffs' and Class Members' Private Information; (2) timely notifying Plaintiffs and Class Members of the Data Breach; and (3) maintaining complete and accurate records of what and where PRC-Saltillo's customers' Private Information was and is stored.

231. PRC-Saltillo had a fiduciary duty to act for the benefit of Plaintiffs and the Class upon matters within the scope of its customers' relationship, in particular to keep the Private Information secure.

232. PRC-Saltillo breached its fiduciary duties to Plaintiffs and the Class by failing to protect their Private Information.

233. PRC-Saltillo breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic PHI PRC-Saltillo created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

234. PRC-Saltillo breached its fiduciary duties to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

235. PRC-Saltillo breached its fiduciary duties to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

236. PRC-Saltillo breached its fiduciary duties to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

237. PRC-Saltillo breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 CFR 164.306(a)(2).

238. PRC-Saltillo breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

239. PRC-Saltillo breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 CFR 164.306(a)(94).

240. PRC-Saltillo breached its fiduciary duties to Plaintiffs and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

241. As a direct and proximate result of PRC-Saltillo's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer the harms and injuries alleged herein, as well as anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT VIII
BREACH OF CONFIDENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR
ALTERNATIVELY THE ILLINOIS SUBCLASS)

242. Plaintiffs restate and reallege all allegations stated above as if fully set forth herein.

243. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by PRC-Saltillo and ultimately accessed and acquired in the Data Breach.

244. As a healthcare devices and services provider, PRC-Saltillo has a special, fiduciary relationship with its customers, including Plaintiffs and Class Members. Because of that special relationship, PRC-Saltillo was provided with and stored Plaintiffs' and Class Members' Private Information and had a duty to maintain such Information in confidence.

245. Customers like Plaintiffs and Class Members have a privacy interest in personal medical and other matters, and PRC-Saltillo had a duty not to disclose such matters concerning its customers.

246. As a result of the parties' relationship, PRC-Saltillo had possession and knowledge of highly sensitive and confidential PHI and PII belonging to Plaintiffs and Class Members, information that was not generally known.

247. Plaintiffs and Class Members did not consent nor authorize Defendant to release or disclose their Private Information to an unknown criminal actor.

248. PRC-Saltillo breached its duty of confidence owed to Plaintiffs and Class Members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of Plaintiffs' and Class Members' Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement adequate information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its customers; and (h) making an unauthorized and unjustified disclosure and release of Plaintiffs' and Class members' Private Information to a criminal third party.

249. But for PRC-Saltillo's wrongful breach of its duty of confidence owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

250. As a direct and proximate result of PRC-Saltillo's wrongful breach of its duty of confidence, Plaintiffs and Class Members have suffered and will continue to suffer the injuries alleged herein.

251. It would be inequitable for PRC-Saltillo to retain the benefit of controlling and maintaining Plaintiffs' and Class Members' Private Information at the expense of Plaintiffs and Class Members.

252. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT IX
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR
ALTERNATIVELY THE ILLINOIS SUBCLASS)

253. Plaintiffs restate and reallege all allegations stated above as if fully set forth herein.

254. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations and state statute described in this Complaint.

255. PRC-Saltillo owes a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs' and Class Members' Private Information.

256. PRC-Saltillo still possesses Private Information regarding Plaintiffs and Class Members.

257. Plaintiffs allege that PRC-Saltillo's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

258. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. PRC-Saltillo owes a legal duty to secure its customers' Private Information and to timely notify customers of a data breach under the common law, HIPAA, the FTCA;
- b. PRC-Saltillo's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect customers' Private Information; and
- c. PRC-Saltillo continues to breach this legal duty by failing to employ reasonable measures to secure customers' Private Information.

259. This Court should also issue corresponding prospective injunctive relief requiring PRC-Saltillo to employ adequate security protocols consistent with legal and industry standards to protect customers' Private Information, including the following:

- a. Order PRC-Saltillo to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.
- b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, PRC-Saltillo must implement and maintain reasonable security measures, including, but not limited to:
 - i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on PRC-Saltillo's systems on a periodic basis, and ordering PRC-Saltillo to promptly correct any problems or issues detected by such third-party security auditors;

- ii. engaging third-party security auditors and internal personnel to run automated security monitoring;
- iii. auditing, testing, and training its security personnel regarding any new or modified procedures;
- iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of PRC-Saltillo's systems;
- v. conducting regular database scanning and security checks;
- vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
- vii. meaningfully educating its customers about the threats they face with regard to the security of their Private Information, as well as the steps they should take to protect themselves.

260. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at PRC-Saltillo. The risk of another such breach is real, immediate, and substantial. If another breach at PRC-Saltillo occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

261. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to PRC-Saltillo if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of PRC-Saltillo's compliance with an injunction requiring reasonable prospective data security

measures is relatively minimal, and PRC-Saltillo has a pre-existing legal obligation to employ such measures.

262. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at PRC-Saltillo, thus preventing future injury to Plaintiffs and other customers whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek the following relief:

- a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class and Illinois Subclass requested herein;
- b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;
- c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;
- d. An order instructing PRC-Saltillo to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;
- e. An order requiring PRC-Saltillo to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

- f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and
- g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

DATED: October 7, 2024

Respectfully submitted,

/s/ Terence R. Coates
Terence R. Coates (0085579)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, Ohio 45202
Telephone: (513) 651-3700
Facsimile: (513) 665-0219
tcoates@msdlegal.com

Tyler J. Bean (*pro hac vice* to be filed)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: tbean@sirillp.com

Attorneys for Plaintiffs and the Putative Classes